

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Yasuyuki HIGASHIURA, et al.**

Group Art Unit: **Not Yet Assigned**

Serial No.: **Not Yet Assigned**

Examiner: **Not Yet Assigned**

Filed: **January 30, 2004**

For: **ELECTRONIC DATA STORAGE SYSTEM AND METHOD THEREOF**

CLAIM FOR PRIORITY UNDER 35 U.S.C. 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Date: January 30, 2004

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

Japanese Appln. No. 2003-25462, filed February 3, 2003


In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicants have complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,

ARMSTRONG, KRATZ, QUINTOS,
HANSON & BROOKS, LLP


William L. Brooks

Attorney for Applicants
Reg. No. 34,129

WLB/jaz
Atty. Docket No. **040033**
Suite 1000
1725 K Street, N.W.
Washington, D.C. 20006
(202) 659-2930



23850

PATENT TRADEMARK OFFICE

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 2 月 3 日

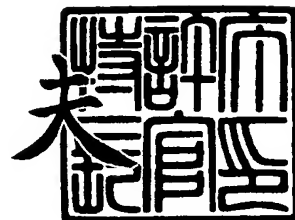
出 願 番 号
Application Number: 特 願 2 0 0 3 - 0 2 5 4 6 2
[ST. 10/C]: [J P 2 0 0 3 - 0 2 5 4 6 2]

出 願 人
Applicant(s): 富士通株式会社
富士通フロンテック株式会社

2 0 0 3 年 1 1 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 0253219

【提出日】 平成15年 2月 3日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60

【発明の名称】 電子データ保管システム及びその方法

【請求項の数】 5

【発明者】

【住所又は居所】 東京都稲城市矢野口 1 7 7 6 番地 富士通フロンテック株式会社内

【氏名】 東浦 康之

【発明者】

【住所又は居所】 東京都稲城市矢野口 1 7 7 6 番地 富士通フロンテック株式会社内

【氏名】 岸野 琢己

【発明者】

【住所又は居所】 東京都稲城市矢野口 1 7 7 6 番地 富士通フロンテック株式会社内

【氏名】 佐藤 啓三

【発明者】

【住所又は居所】 東京都稲城市矢野口 1 7 7 6 番地 富士通フロンテック株式会社内

【氏名】 門脇 昭貴

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 小谷 誠剛

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000237639

【氏名又は名称】 富士通フロンテック株式会社

【代理人】

【識別番号】 100094514

【弁理士】

【氏名又は名称】 林 恒徳

【選任した代理人】

【識別番号】 100094525

【弁理士】

【氏名又は名称】 土井 健二

【手数料の表示】

【予納台帳番号】 030708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【包括委任状番号】 0210821

【プルーフの要否】 要

【書類名】 明細書**【発明の名称】 電子データ保管システム及びその方法****【特許請求の範囲】**

【請求項 1】 少なくとも、電子データを保管するファイル装置と、

電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データおよび公開鍵ベースの電子署名にそれぞれ改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記それぞれのチェックコードを保管し、前記電子データの出力時に、前記保管している電子データと前記電子署名に付与している前記チェックコードにより、それぞれの正当性の検証を行った後、前記電子データと前記電子署名を取り出すデータ処理ユニットとを有することを

特徴とする電子データ保管システム。

【請求項 2】 少なくとも電子データを保管するファイル装置と、

前記電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、公開鍵ベースの電子署名に対して改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記電子署名に対する改ざんチェックコードを保管し、前記電子データの取り出し時に、前記電子署名に付随したチェックコードで前記電子署名の正当性を検証した後、前記電子署名により、前記電子データの正当性の検証を行った後、前記電子データと前記電子署名を取り出すデータ処理ユニットとを有することを

特徴とする電子データ保管システム。

【請求項 3】 前記データ処理ユニットは、前記電子データ、前記電子署名の正当性検証の後、取り出す電子データと登録時電子署名のうち少なくとも一方に対して、取り出し時点の公開鍵ベースの電子署名を付与して出力する

ことを特徴とする請求項 1 又は 2 の電子データ保管システム。

【請求項 4】 電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データおよび公開鍵ベースの電子署名にそれぞれ改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記それぞれのチェックコードを保管するステップと、

前記電子データの取り出し時に、前記保管している電子データと前記電子署名に付与している前記チェックコードにより、それぞれの正当性の検証を行った後、前記電子データと前記電子署名を出力するステップを有することを特徴とする電子データ保管方法。

【請求項 5】 電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、公開鍵ベースの電子署名に対して改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記電子署名に対する改ざんチェックコードを保管するステップと、

前記電子データの取り出し時に、前記電子署名に付随したチェックコードで前記電子署名の正当性を検証した後、前記電子署名により、前記電子データの正当性の検証を行った後、前記電子データと前記電子署名を取り出すステップとを有することを

特徴とする電子データ保管方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、各種文書やデータを電子情報として流通するための電子データ保管システム及びその方法に関し、特に、容易に改ざんでき、また、改ざんが分からない電子データの保管に対して、原本性を確保するための電子データ保管システム及びその方法に関する。

【0 0 0 2】

【従来の技術】

近年の各種のシステムの電子化に伴い、紙ベースのデータが電子化されつつある。電子化されたデータは、容易に改ざん可能であり、且つ改ざんされても容易に判明できない場合がある。このため、電子データの保管にあたっては、電子データが原本として、効力をもつ原本性が要求される。

【0 0 0 3】

このため、電子データの保管として、改ざん検出機能を持つこと、全てのアクセス履歴をとることが有効であり、一般的には、公開鍵ベースの電子署名を使用

して、保管しているデータの原本性を確保し、第三者の検証を可能とすることが行われている。

【0 0 0 4】

近年のコンピュータ技術の発展及びその知識の普及に伴い、電子署名の改ざんの可能性が指摘され、電子署名の長期保存技術により、電子データの原本性を長期に保証する方法が提案されている。

【0 0 0 5】

図 1 3 は、第 1 の従来技術の説明図である。電子データ保管システム 1 0 0 は、登録時の電子データ A に公開鍵ベースの電子署名を付与して保管する。例えば、周知の R S A 暗号化方式では、公開鍵と秘密鍵とのペアを作成し、公開鍵は、C A (Certification Authority) 局 1 1 0 に、オンライン又はフロッピー等によるオフライン形式で、持ち込み、C A 局 1 1 0 から公開鍵証明書 1 0 6 を得る。

【0 0 0 6】

電子データ保管システム 1 0 0 は、公開鍵証明書を得ると、登録する電子データ A のハッシュ値を秘密鍵で R S A 暗号化し、電子署名 P を作成する。この電子署名 P を、電子データ A とともに保管する。電子データ A のアクセスを承認された者には、公開鍵を公開する。秘密鍵で暗号化された電子署名は、公開鍵で復号でき、第 3 者は、電子署名により、電子データの原本性を確認できる。

【0 0 0 7】

この公開鍵証明書に有効期間を設け、有効期限が切れる前に、新規の公開鍵を作り、その鍵により、新たに公開鍵証明書を取得し、電子データ及び電子署名 P を秘密鍵で暗号化し、電子署名 P 1 を作成する。

【0 0 0 8】

通常、公開鍵証明書は、1 年程度の有効期限であるため、毎年、電子署名に電子署名を付けることで署名鍵の危殆化を防ぎ、原本性を確保して、電子データの長期保管を実現する（たとえば、特許文献 1 参照）。

【0 0 0 9】

図 1 4 は、第 2 の従来技術の説明図である。図 1 3 と同様に、C A 局 1 1 0 か

ら公開鍵証明書 1 0 6 を受けて、電子データ A に署名 P を付けて保管する。更に、電子データと電子署名のデータのハッシュ値を、T S A (タイムスタンプオーソリティ) 1 1 2 に送り、公証記録としてのタイムスタンプを取得する。このタイムスタンプ T を、電子データ A, 電子署名 P と共に保管する。このことで、電子データの長期保管を実現する。

【 0 0 1 0 】

【特許文献 1】

特開 2 0 0 0 - 5 9 5 3 2 号公報

【 0 0 1 1 】

【発明が解決しようとする課題】

しかしながら、第 1 の従来技術では、毎年、電子署名の上に電子署名を付けることで、署名の長期保存を行なうので、署名鍵を変更する毎に、保存している全電子データに対して、電子署名を付ける作業が発生する。そのため、電子データを多く保管する保管システムでは、一度に時間がかかりすぎ、運用上の問題となり、現実的には処理が難しい。

【 0 0 1 2 】

又、第 2 の従来技術では、T S A 1 1 2 を外部に持つために、長期保証については、T S A 1 1 2 の責任となる。しかし、T S A 1 1 2 は、第三者機関などが運営するため、使用するための費用が発生する。例えば、電子文書 1 件 x x x 円とか、年間 x x 万円などの費用が発生し、運用コストが増大する。

【 0 0 1 3 】

従って、本発明の目的は、簡易な運用で、且つ新たな費用を発生させずに電子署名の長期保存を実現するための電子データの保管システム及びその方法を提供することにある。

【 0 0 1 4 】

又、本発明の他の目的は、暗号鍵の安全性の問題から、有効期限を持つ公開鍵証明書による電子署名の検証を、有効期限以降、または、失効以降も実行するための電子データ保管システム及びその方法を提供することにある。

【 0 0 1 5 】

更に、本発明の他の目的は、方式／鍵を公開しないより安全な改ざん検出方法による、電子署名とは別の改ざん検出機構を持つことで、電子署名も改ざんされていないことを保証し、電子署名を長期に有効とするための電子データ保管システム及びその方法を提供することにある。

【0016】

更に、本発明の他の目的は、取り出し時に取り出し時点の電子署名を付与することで、電子データの保管システム内で保証した電子データ、登録時署名の検証を第三者が行うことを可能とし、電子データの保管システム以降の出力ルートでの改変を検出するための電子データ保管システム及びその方法を提供することにある。

【0017】

更に、本発明の他の目的は、署名付与時点の公開鍵証明書や失効情報を、電子署名を付与するタイミングで、保管または出力することで、有効期限以降でも第三者が電子署名を検証し、電子文書の正当性を検証するための電子データ保管システム及びその方法を提供することにある。

【0018】

【課題を解決するための手段】

この目的の達成のため、本発明の電子データ保管システムは、少なくとも、電子データを保管するファイル装置と、電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データおよび公開鍵ベースの電子署名にそれぞれ改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記それぞれのチェックコードを保管し、前記電子データの出力時に、前記保管している電子データと前記電子署名に付与している前記チェックコードにより、それぞれの正当性の検証を行った後、前記電子データと前記電子署名を取り出すデータ処理ユニットとを有する。

【0019】

又、本発明の電子データ保管方法は、電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データおよび公開鍵ベースの電子署名にそれぞれ改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵

ベースの電子署名、前記それぞれのチェックコードを保管するステップと、前記電子データの出力時に、前記保管している電子データと前記電子署名に付与している前記チェックコードにより、それぞれの正当性の検証を行った後、前記電子データと前記電子署名を取り出すステップを有する。

【 0 0 2 0 】

本発明では、電子データ保管システム内で、電子データ及び電子署名に対し、非公開であるシステム固有の方式、鍵によるチェックコードを付し、電子文書の取り出し時にチェックするため、電子データ保管システム内で、電子データ及び電子署名の改ざんをチェック、即ち、電子データと電子署名の正常性を確認でき、長期に渡り、電子署名を保証できる。

【 0 0 2 1 】

又、本発明では、少なくとも電子データを保管するファイル装置と、前記電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データ及び公開鍵ベースの電子署名の一方に対して改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記電子署名に対する改ざんチェックコードを保管し、前記電子データの取り出し時に、前記電子署名に付随したチェックコードで前記電子署名の正当性を検証した後、前記電子署名により、前記電子データの正当性の検証を行った後、前記電子データと前記電子署名を取り出すデータ処理ユニットとを有する。

【 0 0 2 2 】

この本発明では、公開鍵証明書の有効期限以降も、独自チェックにより、電子データ及び電子署名の正当性を確保する他に、第 3 者が電子データと登録時電子署名の正当性検証が可能となる。

【 0 0 2 3 】

又、本発明では、好ましくは、前記データ処理ユニットは、前記電子データ、前記電子署名の正当性検証の後、前記電子データと登録時電子署名のうち少なくとも一方に対して、取り出し時点の公開鍵ベースの電子署名を付与して出力する。このように、電子データとともに、登録時電子署名と取り出し時電子署名とを出力するため、第 3 者は、有効な署名鍵を使用して、改ざんチェック（正当性チ

エック)を行うことができる。更に、登録時電子署名を使用して、改ざんチェックでき、これらを使い分けることができる。

【0 0 2 4】

又、本発明では、好ましくは、前記データ処理ユニットは、前記電子署名を作成する場合は、前記電子署名の他に、前記電子署名を作成した公開鍵の証明書を同時に保管する。

【0 0 2 5】

又、本発明では、好ましく、データ処理ユニットは、前記公開鍵証明書の失効情報も同時に保管または出力する。

【0 0 2 6】

更に、本発明では、好ましくは、前記データ処理ユニットは、鍵作成依頼に応じて、前記公開鍵と前記秘密鍵のペアを作成し、前記公開鍵証明書の発行依頼を C A 局に発行し、前記公開鍵証明書を取得し、前記ファイル装置に保管する。

【0 0 2 7】

【発明の実施の形態】

以下、本発明の実施の形態を、電子データ保管システム、電子データの保管及び取り出し処理、他の実施の形態の順で説明するが、本発明は、下記実施の形態に限られない。

【0 0 2 8】

〔電子データ保管システム〕

図 1 は、本発明の一実施の形態の電子データ保管システムの構成図である。図 1 に示すように、複数のクライアント (P C : Personal Computer) 2 - 1 ~ 2 - 4 は、文書作成等の処理を行う。この複数のクライアント 2 - 1 ~ 2 - 4 は、L A N (Local Area Network) 3 で、業務サーバ 1 に接続されており、データ保管やデータ取り出し等を依頼する。

【0 0 2 9】

この L A N 3 には、電子データ保管システム 5 と、その管理クライアント 4 とが接続されている。電子データ保管システム 5 は、電子データを保管 (記憶) するファイル装置 7 と、ファイル制御を行う C P U 6 とからなる。ファイル装置 7

は、必要とするデータ格納容量に応じて、単数又は複数のハードディスク装置で構成される。又、光ディスク装置や光磁気ディスク装置等の他の記憶デバイスで構成しても良い。

【0030】

管理クライアント4は、電子データの管理を行うものであり、CA (Certification Authority) 局8へ公開鍵証明書12の要求を行う。ファイル装置7には、電子データ、電子署名、チェックコード10が、電子文書単位で格納される。又、ファイル装置7には、取得した公開鍵証明書12、生成した公開鍵、秘密鍵のペア14、公開鍵証明書の失効リスト16、CA局証明書18が、格納される。

【0031】

クライアント2-1～2-4は、業務サーバ1に電子データ保管システム5への電子データの保管依頼、電子データの取り出し依頼を行う。又、管理クライアント4は、他のクライアント2-1～2-4と同様に、業務サーバ1に依頼を行うこともできる。

【0032】

管理クライアント4は、CA局8とオンライン又はオフラインで接続し、公開鍵証明書の取得を行う。本発明では、後述するように、電子データ保管システム5が、方式／鍵を公開しないより安全な改ざん方法で、電子署名と別の改ざん検出機構を持ち、電子署名も改ざんされていないことを保証し、電子署名を長期に有効とする。

【0033】

[電子データの保管及び取り出し処理]

次に、図1の構成における電子データの保管及び取り出し処理を説明する。先ず、公開鍵証明書取得処理を、図4の説明図を使用し、図2の処理フロー図により説明する。

【0034】

(S10) 先ず、管理クライアント4は、電子データ保管システム5に鍵作成依頼を行う。

【 0 0 3 5 】

(S 1 2) 電子データ保管システム 5 は、署名鍵（公開鍵と秘密鍵との鍵ペア） 1 4 を作成する。そして、この署名鍵 1 4 をファイル装置 7 に保管する。次に、電子データ保管システム 5 は、公開鍵により、公開鍵証明書要求を作成し、管理クライアント 4 に、応答として、公開鍵証明書要求を返却する。

【 0 0 3 6 】

(S 1 4) 管理クライアント 4 は、電子データ保管システム 5 で作成した公開鍵証明書要求を受け、公開鍵証明書要求をつけて、公開鍵証明書の発行依頼を、C A 局 8 に行う。

【 0 0 3 7 】

(S 1 6) C A 局 8 は、持ち込まれた発行依頼から公開鍵証明書を発行し、管理クライアント 4 は、この公開鍵証明書 1 2 を取得する。

【 0 0 3 8 】

(S 1 8) 管理クライアント 4 は、電子データ保管システム 5 に、公開鍵証明書の登録依頼を行う。電子データ保管システム 5 は、この公開鍵証明書 1 2 をファイル装置 7 に保管する。そして、管理クライアント 4 に処理完了を報告する。これにより、公開鍵証明書取得処理を終了する。

【 0 0 3 9 】

次に、失効情報の取得と登録処理を、図 4 を用いて、図 3 の処理フロー図により説明する。

【 0 0 4 0 】

(S 2 0) 管理クライアント 4 は、定期的に（証明書失効情報には、次の失効情報提供時期が記載されているため、その記載により）C A 局 8 から失効情報の取得要求を行う。

【 0 0 4 1 】

(S 2 2) C A 局 8 は、失効情報の取得要求に応じて、失効情報を管理クライアント 4 に公開し、管理クライアント 4 は、この失効情報 1 6 を取得する。

【 0 0 4 2 】

(S 2 4) 管理クライアント 4 は、電子データ保管システム 5 に、失効情報の

登録を依頼し、電子データ保管システム 5 は、この失効情報 1 6 をファイル装置 4 に登録する。そして、失効情報の取得及び登録処理を終了する。尚、電子署名を作成する場合は、最新の失効情報を確認して、証明書が失効していないことを確認する。

【 0 0 4 3 】

次に、文書の登録処理を、図 6 の文書登録処理の説明図を参照して、図 5 の文書登録処理フロー図により説明する。

【 0 0 4 4 】

(S 3 0) クライアント 2 - 1 ~ 2 - 4 は、業務サーバ 1 を介し電子データ保管システム 5 に、電子データの登録依頼を発行する。

【 0 0 4 5 】

(S 3 2) 電子データ保管システム 5 は、電子データ A を受け付け、電子データ A のハッシュ値からシステム固有の暗号化アルゴリズムにより、改ざん検出チェックコード C (A) を作成する。

【 0 0 4 6 】

(S 3 4) 電子データ A のハッシュ値を、秘密鍵で R S A 暗号化し、登録時電子署名 P を作成する。更に、電子署名 P のハッシュ値からシステム固有の暗号化アルゴリズムにより、改ざん検出チェックコード C (P) を作成する。

【 0 0 4 7 】

(S 3 6) 電子データ保管システム 5 は、電子データに登録時の電子署名を付け、それぞれのデータにチェックコードを付与して、ファイル装置 7 に保管する。業務サーバ 1 に登録完了を通知する。これにより、文書登録処理を終了する。

【 0 0 4 8 】

次に、文書の取り出し処理を、図 8 の文書取り出し処理の説明図を参照して、図 7 の文書取り出し処理フロー図により説明する。

【 0 0 4 9 】

(S 4 0) クライアント 2 - 1 ~ 2 - 4 は、業務サーバ 1 を介し又は直接、電子データ保管システム 5 に、電子データの取り出し依頼を発行する。

【 0 0 5 0 】

(S 4 2) 電子データ保管システム 5 は、ファイル装置 7 の電子データ A を検索する。

【0051】

(S 4 4) 電子データ保管システム 5 は、電子データ A と電子署名 P を、各々の改ざん検出チェックコード C (A)、C (P) により検証する。即ち、前述と同様に、検索された電子データ A のハッシュ値からシステム固有の暗号化アルゴリズムにより、改ざん検出チェックコード C (A) を作成し、保管されている改ざん検出チェックコード C (A) と比較する。又、検索された登録時電子署名 P のハッシュ値からシステム固有の暗号化アルゴリズムにより、改ざん検出チェックコード C (P) を作成し、保管されている改ざん検出チェックコード C (P) と比較する。

【0052】

(S 4 6) 電子データ保管システム 5 は、検証結果が良好なら、電子データ A のハッシュ値を、取り出し時に有効な公開鍵証明書の秘密鍵で RSA 暗号化し、取り出し時電子署名 P ' を作成する。

【0053】

(S 4 8) 電子データ保管システム 5 は、電子データ A に、登録時の電子署名 P, 取り出し時電子署名 P ' を付け、依頼された業務サーバ 1、クライアント 2-1 ~ 2-4 に出力し、終了する。尚、検証結果が不良なら、改ざんの可能性があるため、出力不可を通知する。

【0054】

電子データを取りだした第 3 者は、公開鍵により、取り出し時電子署名を復号化し、改ざんの有無を検証する。

【0055】

図 9 は、その動作説明図である。ここでは、2001 年、2002 年、2003 年と 1 年毎に、有効な署名鍵が、PK, QK, RK と変更された場合に、2001 年に、文書 A を登録し、登録時の電子署名 P、およびそれぞれのチェックコード C (A), C (P) を保管した例を示す。

【0056】

この例において、電子データ保管システム 5 内で、非公開であるシステム固有のチェックコード C (A) , C (P) を付し、電子文書の取り出し時にチェックするため、電子データ保管システム内で、電子データ及び電子署名の改ざんをチェック、即ち、電子データと電子署名の正常性を確認できる。

【0057】

又、文書取り出し時に、電子データ A とともに、登録時電子署名と取り出し時電子署名とを出力する。例えば、2001 年の文書取り出し時には、電子データ A とともに、登録時電子署名 P と取り出し時電子署名 P とを出力する。2002 年の文書取り出し時には、電子データ A とともに、登録時電子署名 P と取り出し時電子署名 Q とを出力する。2003 年の文書取り出し時には、電子データ A とともに、登録時電子署名 P と取り出し時電子署名 R とを出力する。このため、第三者は、有効な署名鍵を使用して、改ざんチェック（正当性チェック）を行うことができる。更に、登録時電子署名を使用して、改ざんチェックでき、これらを使い分けることができる。

【0058】

このように、公開鍵証明書は、通常 1 年程度が有効期間であり、長期にデータを保管した場合にも、登録時電子署名が、危殆化せず、常に有効となる。尚、有効期限以降の署名検証ができるデータ全てを含む。例えば、電子署名、自公開鍵証明書、CA 局証明書、CRL (CA 局失効情報)、ARL (公開鍵証明書失効情報) を指す。

【0059】

[他の実施の形態]

図 10 は、本発明の他の実施の形態の説明図である。この実施の形態では、取り出し時の電子署名 Q として、登録時電子署名 P のハッシュ値を、取り出し時に有効な公開鍵証明書の秘密鍵で RSA 暗号化し、取り出し時電子署名 Q を作成する。

【0060】

即ち、図 7 及び図 8 の一実施の形態が、取り出し時電子署名を、電子データの暗号化で作成しているが、この実施の形態では、取り出し時電子署名を、登録時

電子署名Pを暗号化して作成している。

【0061】

このため、公開鍵証明書の有効期限以降も、独自チェックにより、電子データ及び電子署名Pの正当性を確保する他に、第3者が電子データと登録時電子署名の正当性検証が可能となる。

【0062】

図11及び図12は、本発明の更に他の実施の形態の説明図である。この実施の形態では、電子データAの登録時に、登録時電子署名PのチェックコードC（P）のみ作成し、電子データA、登録時電子署名P、チェックコードC（P）とを保存する。

【0063】

取り出し時には、登録時電子署名Pに付随したチェックコードC（P）により、登録時電子署名Pの正当性を検証し、その後、電子署名Pにより、電子データAの正当性をチェックする。その後取り出し時電子署名Qとして、電子データ又は登録時電子署名Pのハッシュ値を、取り出し時に有効な公開鍵証明書の秘密鍵でRSA暗号化し、取り出し時電子署名Qを作成する。

【0064】

即ち、図7及び図8の一実施の形態及び図10の他の実施の形態が、登録時に、電子データと、登録時電子署名の各々に作成しているが、この実施の形態では、登録時チェックコードを1つのチェックコードで実現する。

【0065】

このため、同様に、公開鍵証明書の有効期限以降も、独自チェックにより、電子データ及び電子署名Pの正当性を確保する他に、第3者が電子データと登録時電子署名の正当性検証が可能となる。

【0066】

前述の実施の形態では、図1のような構成における電子データ保管システムで説明したが、これ以外の構成における電子データ保管システムに適用できる。又、記憶デバイスは、磁気ディスク、光ディスク、光磁気ディスク、各種のストレージデバイスを適用できる。

【 0 0 6 7 】

又、C A 局を 1 つで説明したが、複数の C A 局や階層化された複数の C A 局で公開鍵証明書を取得することもできる。

【 0 0 6 8 】

以上、本発明を実施の形態により説明したが、本発明の趣旨の範囲内において、本発明は、種々の変形が可能であり、本発明の範囲からこれらを排除するものではない。

【 0 0 6 9 】

(付記 1) 少なくとも、電子データを保管するファイル装置と、電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データおよび公開鍵ベースの電子署名にそれぞれ改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記それぞれのチェックコードを保管し、前記電子データの出力時に、前記保管している電子データと前記電子署名に付与している前記チェックコードにより、それぞれの正当性の検証を行った後、前記電子データと前記電子署名を取り出すデータ処理ユニットとを有することを特徴とする電子データ保管システム。

【 0 0 7 0 】

(付記 2) 少なくとも電子データを保管するファイル装置と、前記電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、公開鍵ベースの電子署名に対して改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記電子署名に対する改ざんチェックコードを保管し、前記電子データの出力時に、前記電子署名に付随したチェックコードで前記電子署名の正当性を検証し、前記電子署名により、前記電子データの正当性の検証を行った後、前記電子データと前記電子署名を取り出すデータ処理ユニットとを有することを特徴とする電子データ保管システム。

【 0 0 7 1 】

(付記 3) 前記データ処理ユニットは、前記電子データ、前記電子署名の正当性検証の後、取り出す登録時電子署名に対して、取り出し時点の公開鍵ベースの電子署名を付与して出力することを特徴とする付記 1 の電子データ保管システム

。

【 0 0 7 2 】

（付記 4）前記データ処理ユニットは、前記電子データ、前記電子署名の正当性検証の後、取り出す電子データに対して、取り出し時点の公開鍵ベースの電子署名を付与して出力することを特徴とする付記 1 の電子データ保管システム。

【 0 0 7 3 】

（付記 5）前記データ処理ユニットは、前記電子データ、前記電子署名の正当性検証の後、取り出す登録時電子署名に対して、取り出し時点の公開鍵ベースの電子署名を付与して出力することを特徴とする付記 2 の電子データ保管システム。

。

【 0 0 7 4 】

（付記 6）前記データ処理ユニットは、前記電子署名を作成する場合は、前記電子署名の他に、前記電子署名を作成した公開鍵の証明書を同時に保管することを特徴とする付記 1 の電子データ保管システム。

【 0 0 7 5 】

（付記 7）前記データ処理ユニットは、前記公開鍵証明書の失効情報も同時に保管または出力することを特徴とする付記 1 の電子データ保管システム。

【 0 0 7 6 】

（付記 8）前記データ処理ユニットは、前記電子署名を作成する場合は、前記電子署名の他に、前記電子署名を作成した公開鍵の証明書を同時に保管することを特徴とする付記 2 の電子データ保管システム。

【 0 0 7 7 】

（付記 9）前記データ処理ユニットは、前記公開鍵証明書の失効情報も同時に保管または出力することを特徴とする付記 2 の電子データ保管システム。

【 0 0 7 8 】

（付記 10）前記データ処理ユニットは、鍵作成依頼に応じて、前記公開鍵と前記秘密鍵のペアを作成し、前記公開鍵証明書の発行依頼を C A 局に発行し、前記公開鍵証明書を取得し、前記ファイル装置に保管することを特徴する付記 1 の電子データ保管システム。

【 0 0 7 9 】

(付記 1 1) 電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データおよび公開鍵ベースの電子署名にそれぞれ改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記それぞれのチェックコードを保管するステップと、前記電子データの出力時に、前記保管している電子データと前記電子署名に付与している前記チェックコードにより、それぞれの正当性の検証を行った後、前記電子データと前記電子署名を取り出すステップを有することを特徴とする電子データ保管方法。

【 0 0 8 0 】

(付記 1 2) 前記電子データ、前記電子署名の正当性検証の後、取り出す登録時電子署名に対して、取り出し時点の公開鍵ベースの電子署名を付与して出力するステップを更に有することを特徴とする付記 1 1 の電子データ保管方法。

【 0 0 8 1 】

(付記 1 3) 電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、前記電子データおよび公開鍵ベースの電子署名にそれぞれ改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記それぞれのチェックコードを保管するステップと、前記電子データの出力時に、前記保管している電子データと前記電子署名に付与している前記チェックコードにより、それぞれの正当性の検証を行った後、前記電子データと前記電子署名を取り出すステップを有することを特徴とする電子データ保管方法。

【 0 0 8 2 】

(付記 1 4) 電子データの登録時に、公開しない暗号方法又は／及び暗号鍵により、公開鍵ベースの電子署名に対して改ざん検出用のチェックコードを生成し、前記電子データ、前記公開鍵ベースの電子署名、前記電子署名に対する改ざんチェックコードを保管するステップと、前記電子データの出力時に、前記電子署名に付随したチェックコードで前記電子署名の正当性を検証した後、前記電子署名により、前記電子データの正当性の検証を行った後、前記電子データと前記電子署名を取り出すステップとを有することを特徴とする電子データ保管方法。

【 0 0 8 3 】

(付記 1 5) 前記電子データ、前記電子署名の正当性検証の後、取り出す登録時電子署名に対して、取り出し時点の公開鍵ベースの電子署名を付与して出力するステップを更に有することを特徴とする付記 1 3 の電子データ保管方法。

【 0 0 8 4 】

(付記 1 6) 前記電子データ、前記電子署名の正当性検証の後、取り出す電子データに対して、取り出し時点の公開鍵ベースの電子署名を付与して出力することを特徴とする付記 1 4 の電子データ保管方法。

【 0 0 8 5 】

(付記 1 7) 前記保管ステップは、前記電子署名を作成する場合は、前記電子署名の他に、前記電子署名を作成した公開鍵の証明書を同時に保管することを特徴とする付記 1 3 の電子データ保管方法。

【 0 0 8 6 】

(付記 1 8) 前記保管ステップは、前記電子署名を作成する場合は、前記電子署名の他に、前記電子署名を作成した公開鍵の証明書を同時に保管することを特徴とする付記 1 4 の電子データ保管方法。

【 0 0 8 7 】

(付記 1 9) 前記保管及び出力ステップは、前記公開鍵証明書の失効情報も同時に保管または出力することを特徴とする付記 1 3 の電子データ保管方法。

【 0 0 8 8 】

(付記 2 0) 鍵作成依頼に応じて、前記公開鍵と前記秘密鍵のペアを作成し、前記公開鍵証明書の発行依頼を C A 局に発行し、前記公開鍵証明書を取得し、前記ファイル装置に保管するステップを更に有することを特徴する付記 1 3 の電子データ保管方法。

【 0 0 8 9 】

(付記 2 1) 保管及び出力ステップは、前記公開鍵証明書の失効情報も同時に保管または出力することを特徴とする付記 1 4 の電子データ保管方法。

【 0 0 9 0 】

(付記 2 2) 鍵作成依頼に応じて、前記公開鍵と前記秘密鍵のペアを作成し、前記公開鍵証明書の発行依頼を C A 局に発行し、前記公開鍵証明書を取得し、前

記ファイル装置に保管するステップを更に有することを特徴する付記 14 の電子データ保管方法。

【0091】

【発明の効果】

このように、本発明では、公開鍵ベースの署名にすることにより、第三者検証が可能となるとともに、公開しないチェックコードを持つことで、登録時の電子署名が、危殆化せず、常に有効となる。

【0092】

又、取り出し時の電子署名を付けることで、保管していたデータに間違いがないことを保証し、また、第三者が検証出来る。

【0093】

更に、これらのことにより、第三者検証を長期に渡り可能とする。電子データの長期保管を実現する（長期間、改変の検出を保証する）。

【図面の簡単な説明】

【図 1】

本発明の一実施の形態の電子データ保管システムの構成図である。

【図 2】

図 1 の公開鍵証明書取得処理フロー図である。

【図 3】

図 1 の公開鍵証明書の取得動作の説明図である。

【図 4】

図 1 の公開鍵失効情報取得処理フロー図である。

【図 5】

図 1 の文書登録処理フロー図である。

【図 6】

図 5 の文書登録処理の動作説明図である。

【図 7】

図 1 の文書取り出し処理フロー図である。

【図 8】

図 8 の文書取り出し処理の説明図である。

【図 9】

図 8 の文書取り出し動作説明図である。

【図 1 0】

本発明の他の実施の形態の説明図である。

【図 1 1】

本発明の更に他の実施の形態の動作説明図である。

【図 1 2】

図 1 1 の処理の動作説明図である。

【図 1 3】

第 1 の従来技術の説明図である。

【図 1 4】

第 2 の従来技術の説明図である。

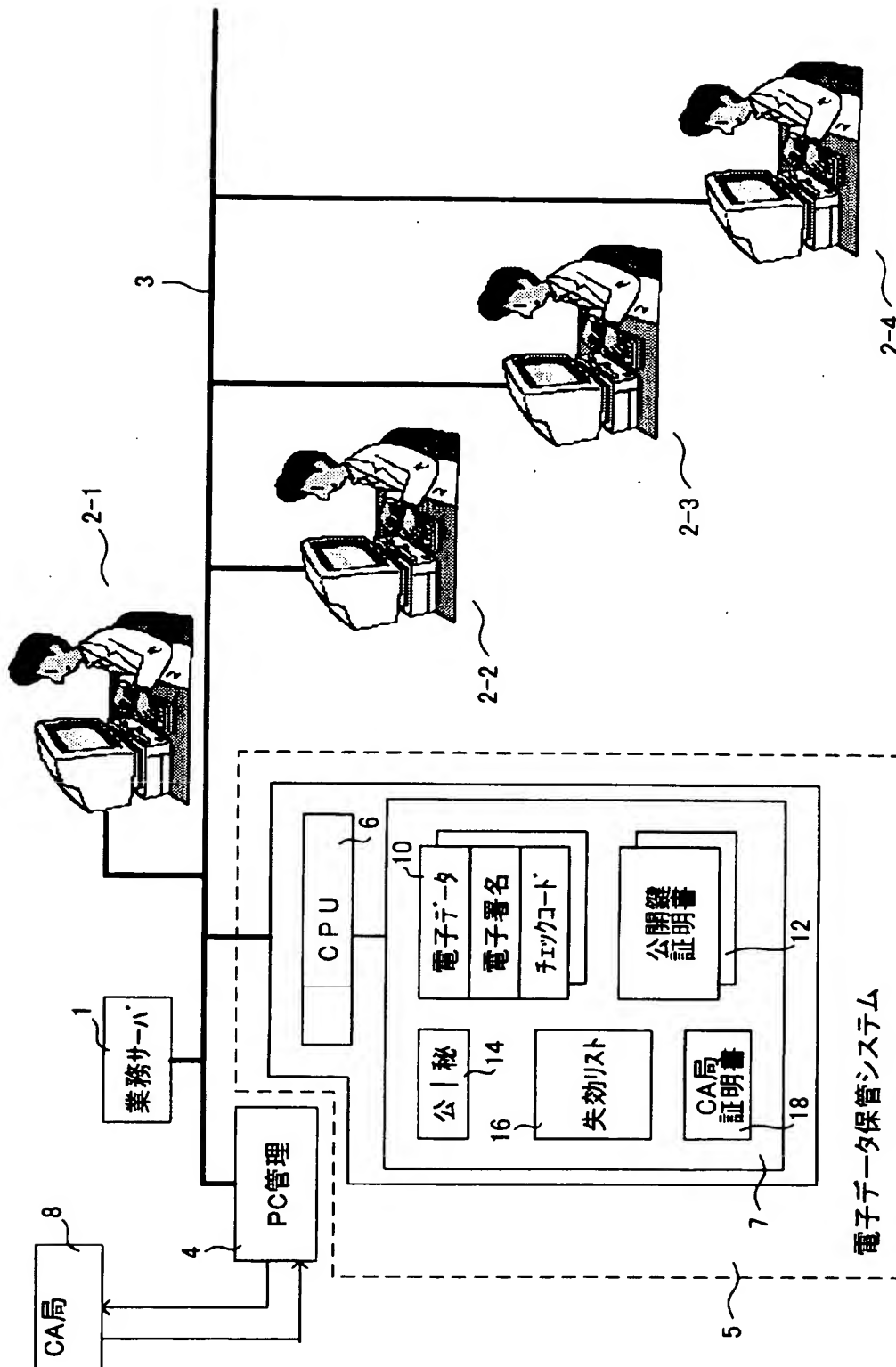
【符号の説明】

- 1 業務サーバ
- 2-1 ~ 2-4 クライアント
- 3 LAN
- 4 管理クライアント
- 5 電子データ保管システム
- 6 CPU
- 7 ファイル装置
- 8 CA局
- 10 電子データ、電子署名、チェックデータ
- 12 公開鍵証明書
- 14 署名鍵
- 16 失効リスト
- 18 CA局証明書

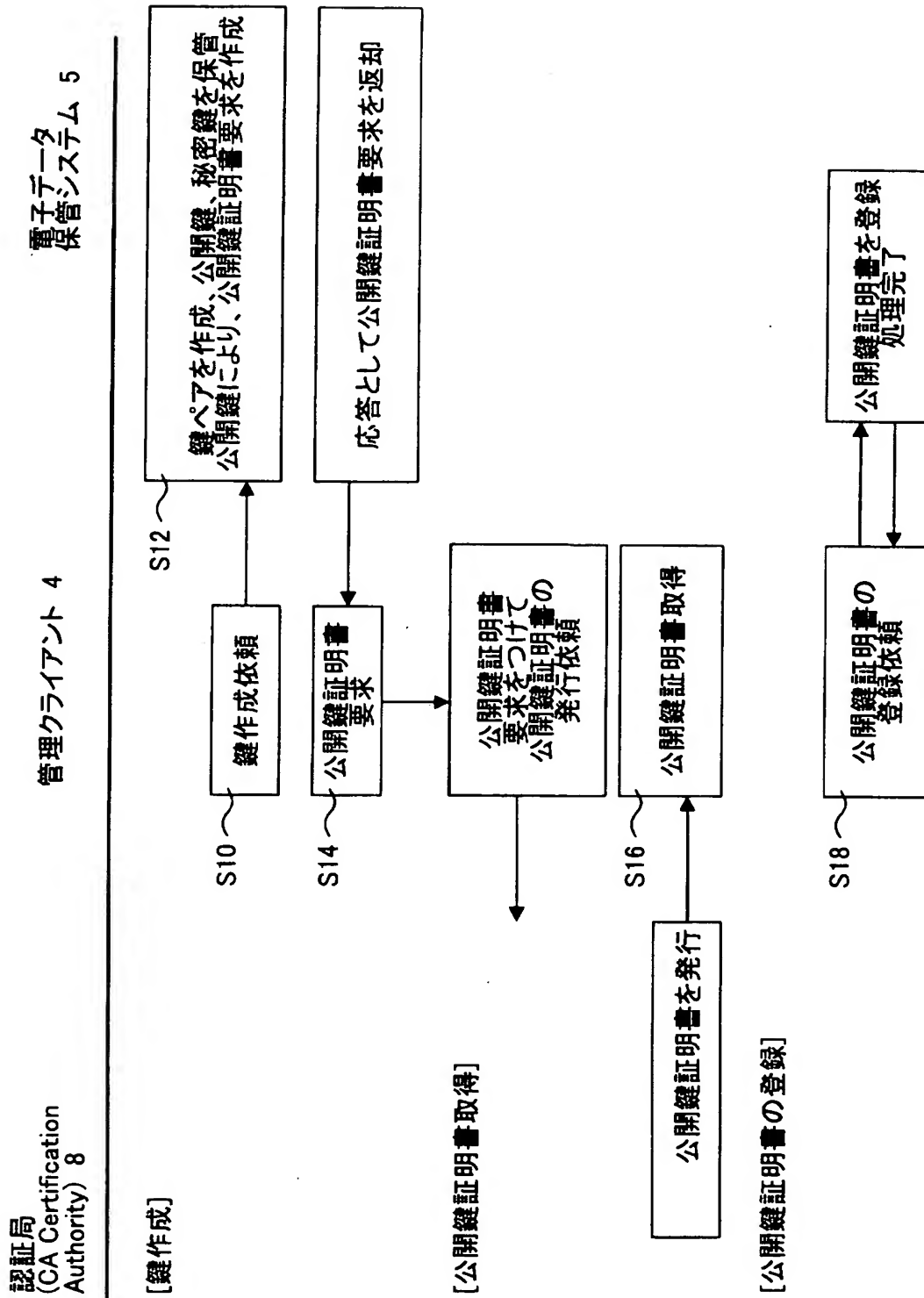
【書類名】

図面

【図 1】



【図 2】



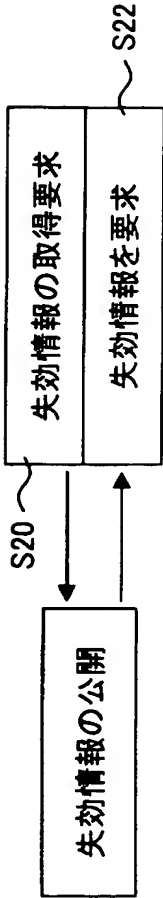
【図 3】

認証局
(CA Certification
Authority) 8

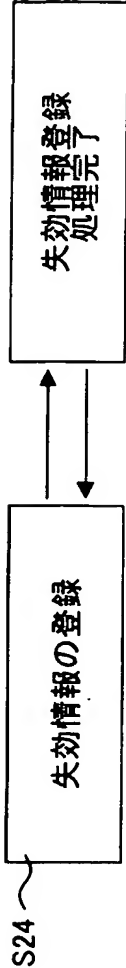
管理クライアント 4

電子データ
保管システム 5

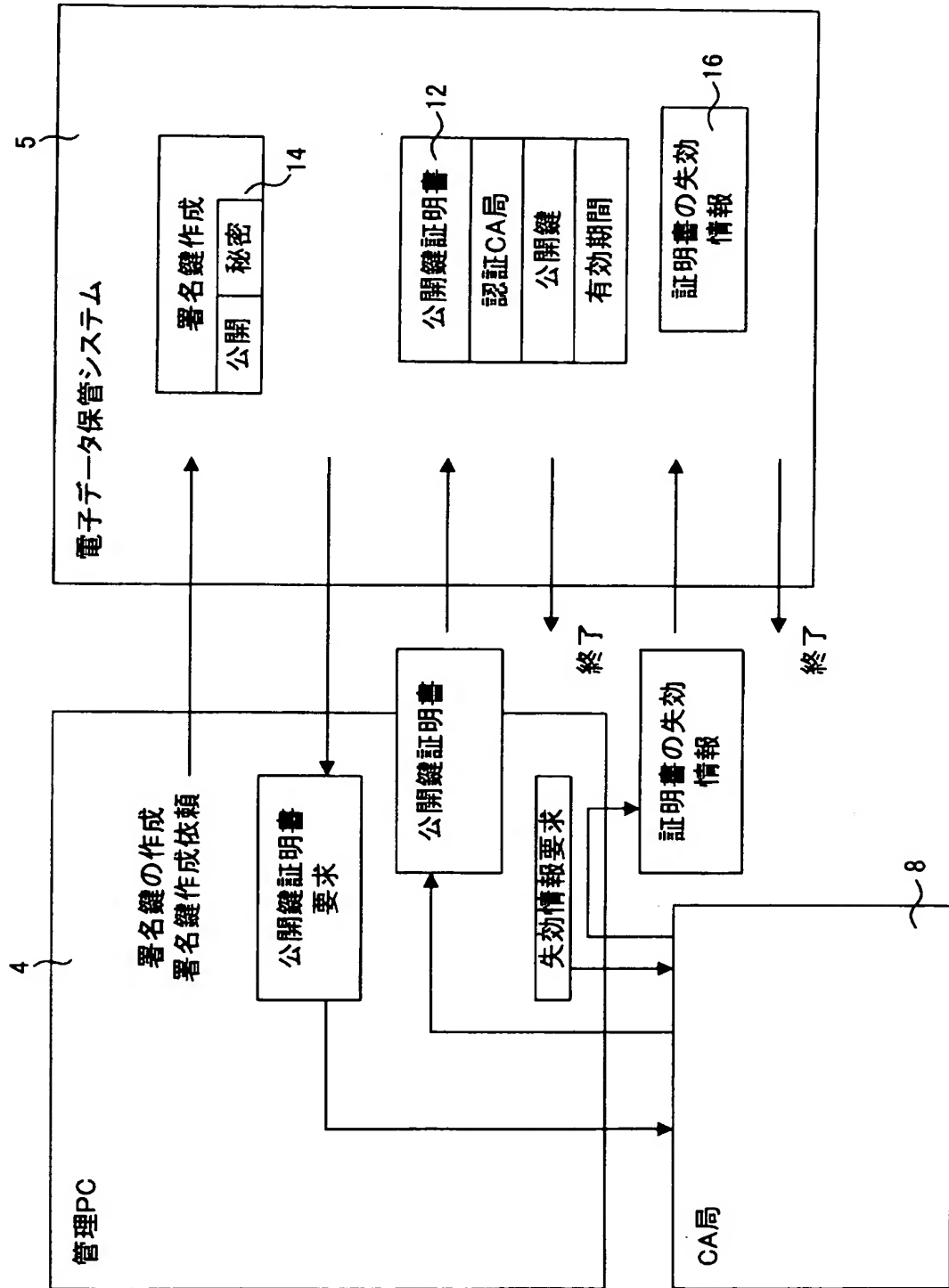
[失効情報取得]



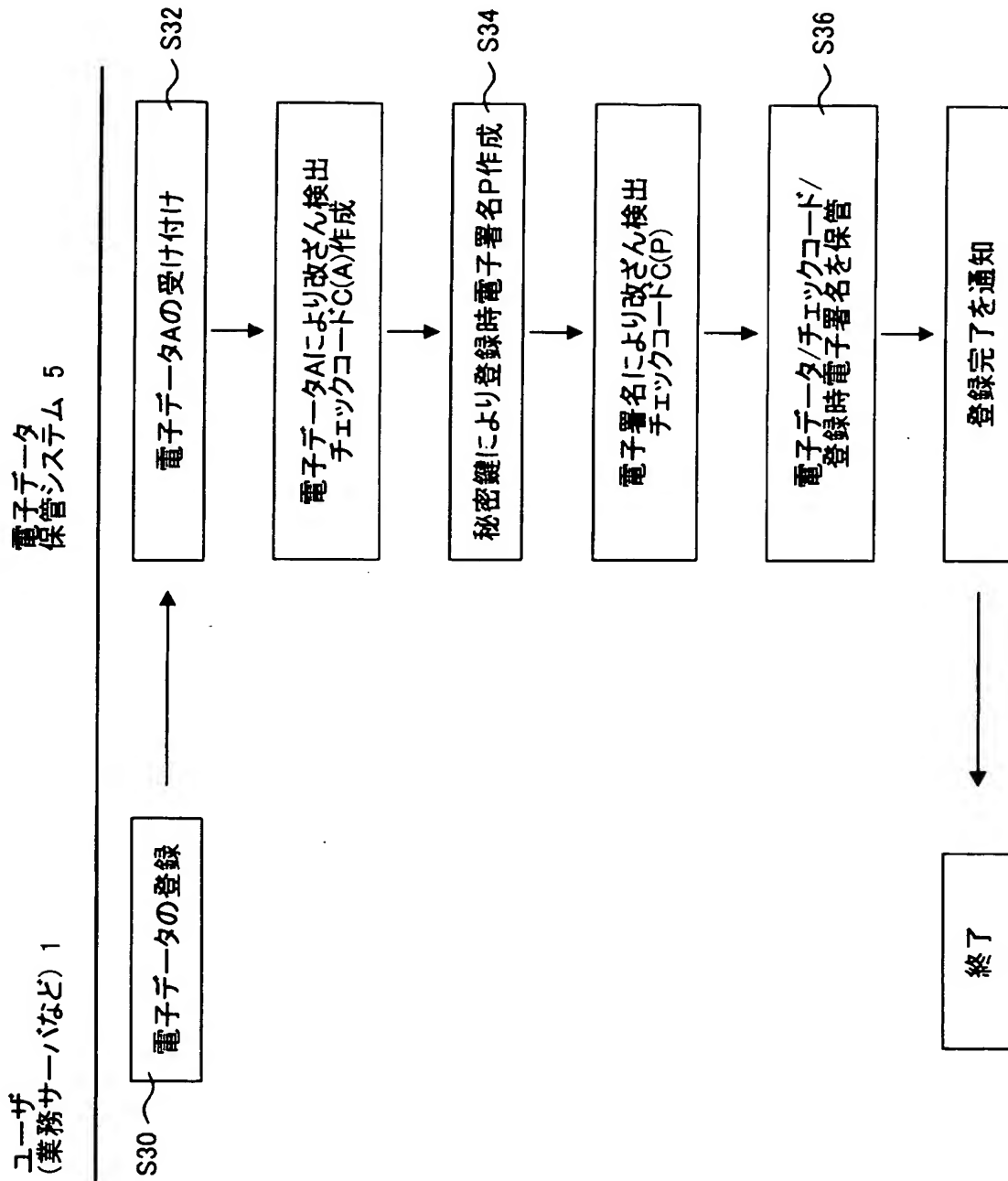
[失効情報の登録]




【図 4】



【図5】



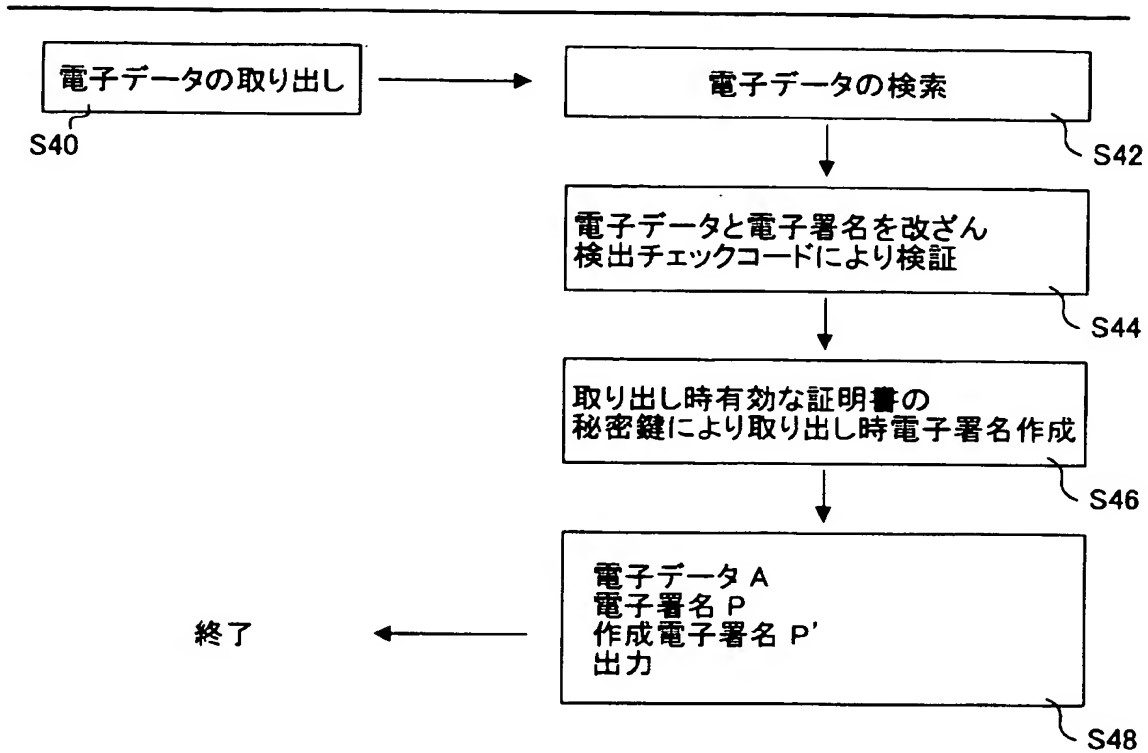
【図 6】

項目	2001年	2002年	2003年	備考
署名鍵	P-K	Q-K	R-K	
文書(A) 格納形態	<div><div>A</div><div>C(A)</div><div>P</div><div>C(P)</div></div>			
文書(A) 取出形態	<div><div>A</div><div>P</div><div>P</div><div>P</div></div>	<div><div>A</div><div>P</div><div>Q</div></div>	<div><div>A</div><div>P</div><div>R</div></div>	

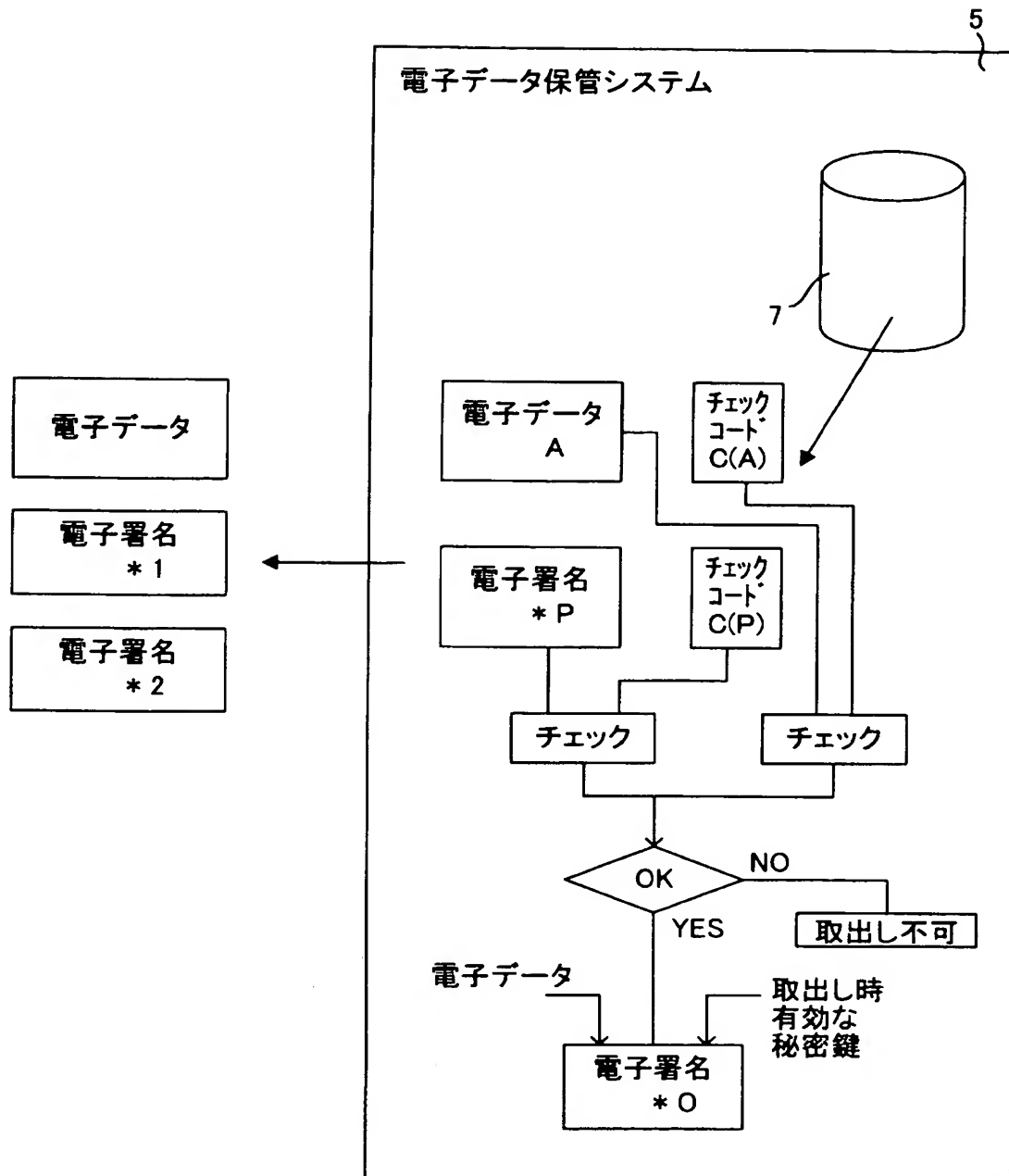
【図 7】

業務サーバ 1, クライアント


電子データ保管システム 8



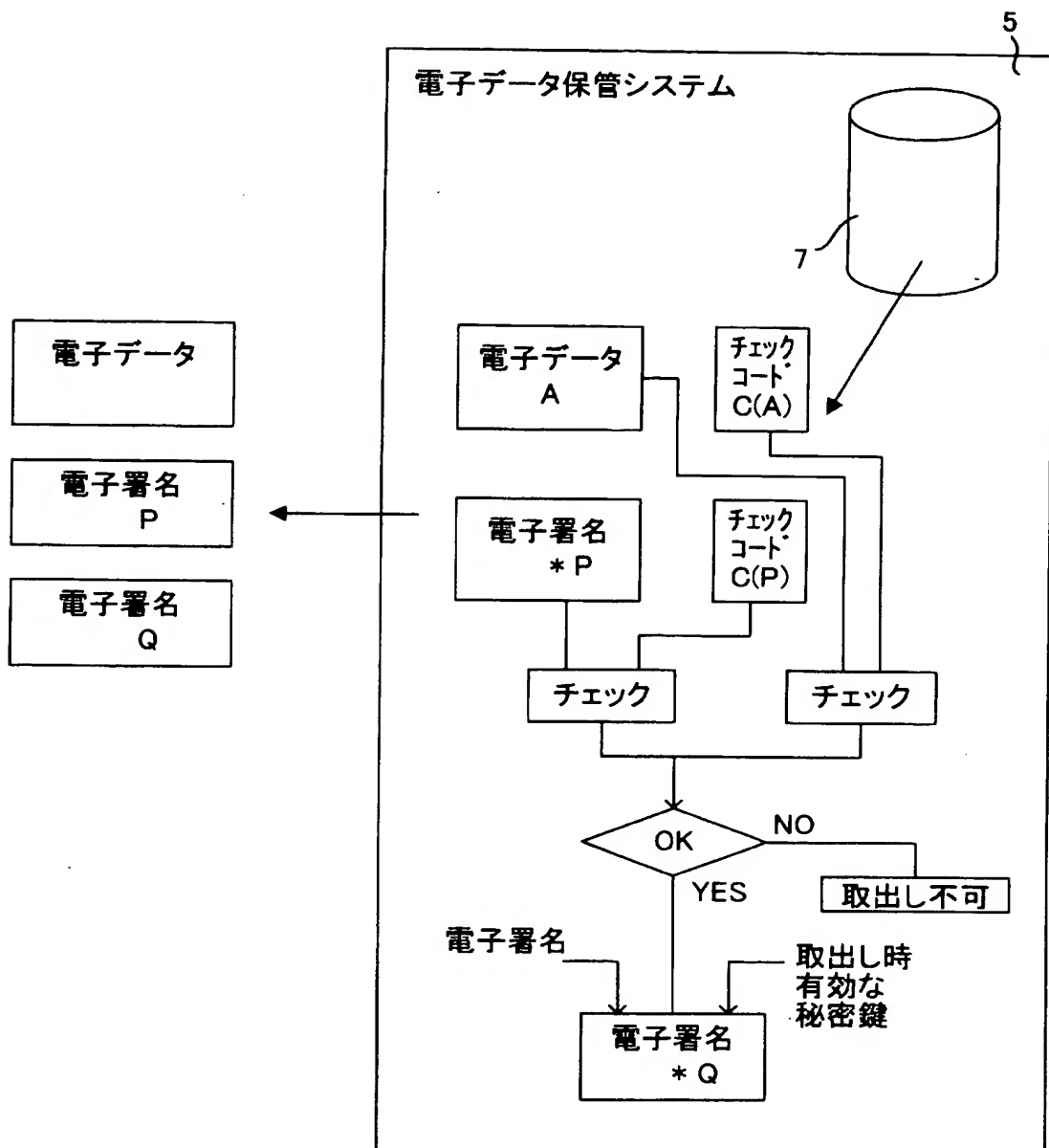
【図 8】



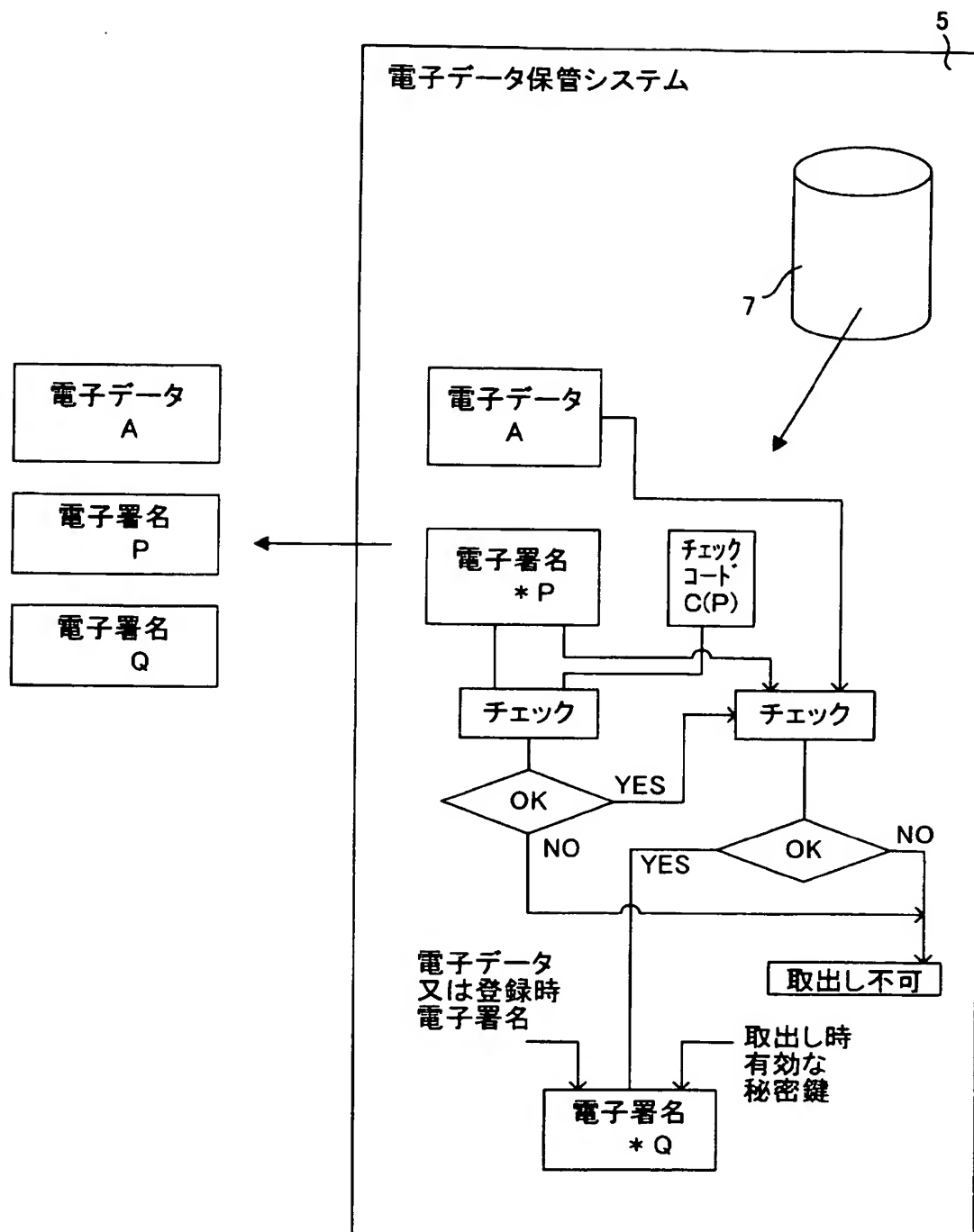
【図 9】

項目	2001年	2002年	2003年	備考
署名鍵	P-K	Q-K	R-K	
文書(A) 格納形態	<div><div>A</div><div>C(A)</div><div>P</div><div>C(P)</div></div>			
文書(A) 取出形態	<div><div>A</div><div>P</div><div>P</div><div>P</div></div>	<div><div>A</div><div>P</div><div>Q</div></div>	<div><div>A</div><div>P</div><div>R</div></div>	


【図 10】



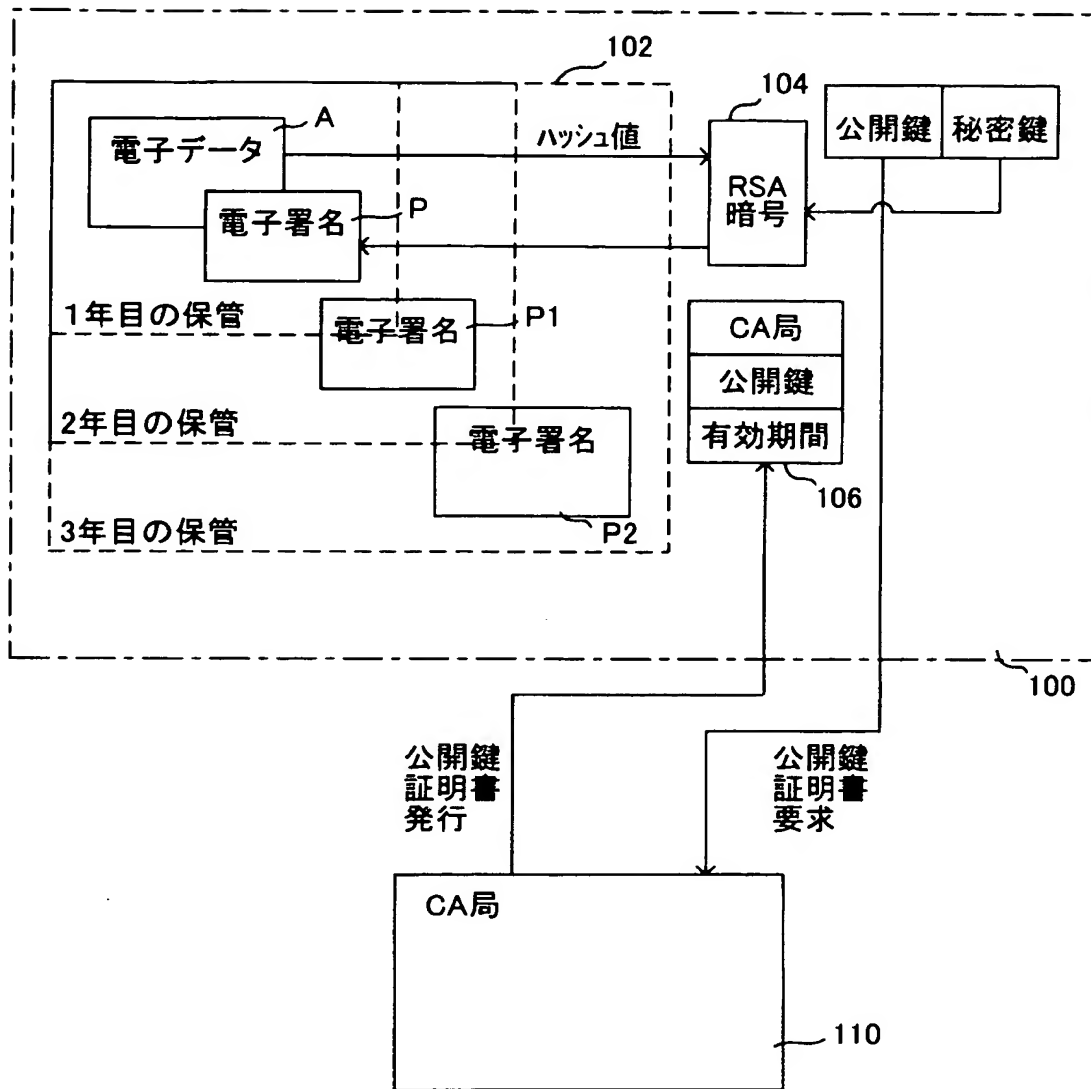
【図 11】



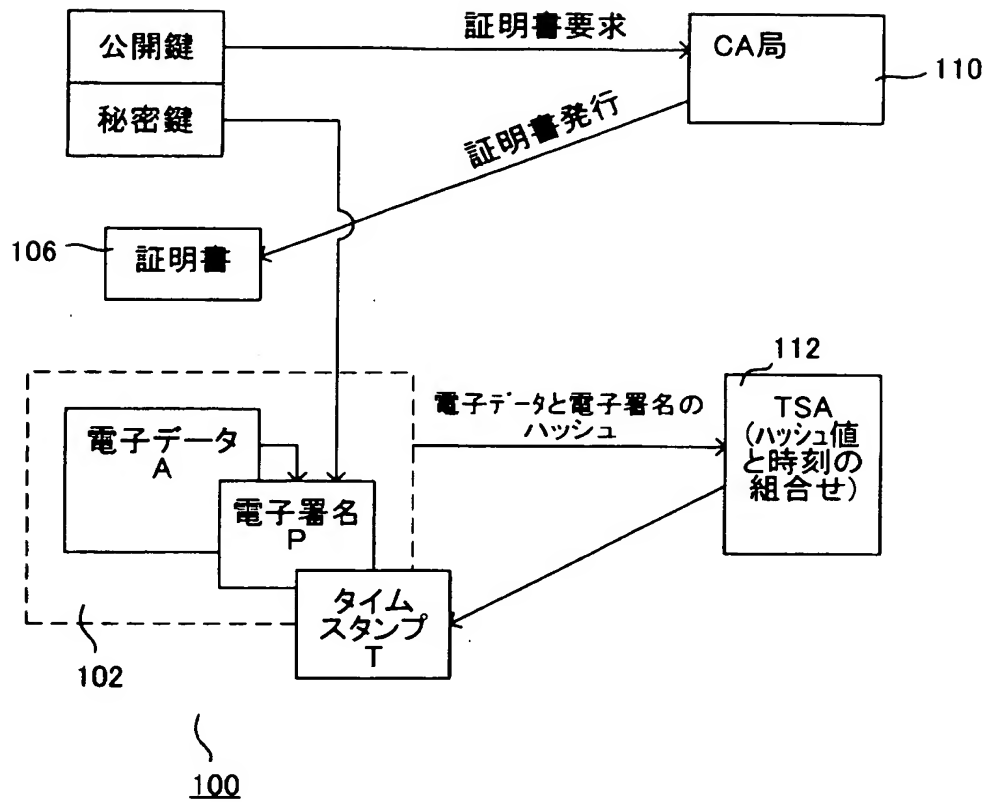
【図 1 2】

項目	2001年	2002年	2003年	備考
署名鍵	P-K	Q-K	R-K	
文書(A) 格納形態	<div>A</div> <div>P</div> <div>C(P)</div>			
文書(A) 取出形態	<div>A</div> <div>P</div> <div>P</div>	<div>A</div> <div>P</div> <div>Q</div>	<div>A</div> <div>P</div> <div>R</div>	

【図 13】



【図 14】



【書類名】 要約書

【要約】

【課題】 電子データに、電子署名を付加して保管し、電子データとともに、電子署名を付加して出力する電子データ保管システムにおいて、簡易な運用でかつ運用コストを低減する。

【解決手段】 公開鍵ベースの署名にすることにより、第三者検証が可能となるとともに、公開しないチェックコードを持つことで、登録時の電子署名が、危殆化せず、常に有効となる。又、取り出し時の電子署名を付けることで、保管していたデータに間違いないことを保証し、また、第三者が検証出来る。更に、これらのことにより、第三者検証を長期に渡り可能とする。電子データの長期保管を実現する。

【選択図】 図 9

特願 2 0 0 3 - 0 2 5 4 6 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社

特願 2 0 0 3 - 0 2 5 4 6 2

出 願 人 履 歴 情 報

識別番号

[0 0 0 2 3 7 6 3 9]

1. 変更年月日

2 0 0 2 年 7 月 9 日

[変更理由]

名称変更

住 所

東京都稲城市矢野口 1 7 7 6 番地

氏 名

富士通フロンテック株式会社